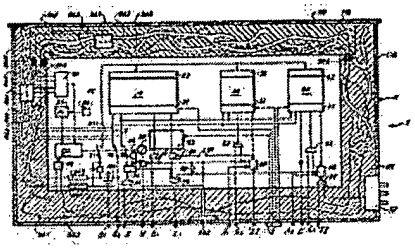
MOBILER DATENBEHAELTER

Publication number: DE3023427 (A1)
Publication date: 1981-01-08
Inventor(s): EHRAT KURT DIPL ING
Applicant(s): GRETAG AG
Classification:
- international: ***G06F21/00; G06K19/073; G07F7/10; H04L9/22;*** **G06F21/00; G06K19/073; G07F7/10; H04L9/18;** (IPC1-7): G06F13/00
- European: G06F21/00N1T1; G06K19/073; G06K19/073A8; G07F7/10D6F; G07F7/10D12; H04L9/22
Application number: DE19803023427 19800623
Priority number(s): CH19790006037 19790628

Also published as:
CH640971 (A5)

Abstract of **DE 3023427 (A1)**

Arranged in a plastic housing (11), which is closed on all sides and is provided with a metal shielding (113), are a main data memory (20) for useful data to be protected against unauthorised access, two identification devices (40, 70; 30, 60) and a system of destruction sensors (941, 942, 961-965) with associated switching stages (90-96). The two identification devices control the electrical access to the main data memory (20) by permitting a writing or reading operation only when a preceding identification process, in which identification information is fed in from outside, was positive. The destruction sensors, which are in particular current and pressure sensors laid in the walls of the container, respond to violent opening of the container housing (11) and initiate via a switching stage (90) erasure of the main data memory (20).



(51) Int. Cl. 3: G 06 F 13/00

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(11) Offenlegungsschrift 30 23 427

(21) Aktenzeichen: P 30 23 427.6

(22) Anmeldetag: 23. 6. 80

(43) Offenlegungstag: 8. 1. 81

(30) Unionspriorität:

(32) (33) (31) 28. 6. 79 Schweiz 6037-79

(54) Bezeichnung: Mobiler Datenbehälter

(71) Anmelder: Gretag AG, Regensdorf, Zürich (Schweiz)

(74) Vertreter: Berg, W.J., Dipl.-Chem. Dr.rer.nat.; Stapf, O., Dipl.-Ing.; Schwabe, H.-G., Dipl.-Ing.; Sandmair, K., Dipl.-Chem. Dr.jur.Dr.rer.nat.; Pat.-Anwälte, 8000 München

(72) Erfinder: Ehrat, Kurt, Dipl.-Ing., Steinmaur (Schweiz)

DE 30 23 427 A 1

12. 80 030 062/838

DR. BERG DIPL.-ING. STAPF
DIPL.-ING. SCHWABE DR. DR. SANDMAIR
PATENTANWÄLTE
8 MÜNCHEN 80 · MAUERKIRCHERSTR. 45

Anwaltsakte: 30 945

3023427

Patentansprüche

1. Mobiler Datenbehälter zur gegen unbefugten Zugriff gesicherten Speicherung von Nutzdaten mit einem abgeschlossenen Gehäuse (11), in welchem sich ein Hauptdatenspeicher (20) für die Nutzdaten und eine Identifikationseinrichtung (40, 70) befinden, welche ihr von aussen zugeführte Identifikationsdaten mit in ihr gespeicherten Identifikationsdaten vergleicht und je nach Vergleichsergebnis den Zugang zum Hauptdatenspeicher (20) freigibt oder blockiert, und welcher Datenbehälter ferner mit Sensormitteln (90-96) ausgestattet ist, die bei gewaltsamem oder unbefugtem Oeffnen des Datenbehälters einen Teil der gespeicherten Daten unbrauchbar machen oder zerstören, dadurch gekennzeichnet, dass die Sensormittel (90-96) die im Hauptdatenspeicher befindlichen Nutzdaten unbrauchbar machen oder löschen.

2. Datenbehälter nach Anspruch 1, dadurch gekennzeichnet, dass die Sensormittel (90-96) in den Wänden (112, 111) des Gehäuses (119 angeordnete Zerstörungssensoren (941, 942; 962-965) umfassen, welche ansprechen, wenn die Wände durchbrochen werden.

3. Datenbehälter nach Anspruch 2, dadurch gekennzeichnet, dass die Sensormittel (90-96) von Datenbehälter zu Datenbehälter verschieden und vorzugsweise zufallsmässig verteilt angeordnet und gegen Lokalisierung von aussen gesichert sind.

4. Datenbehälter nach Anspruch 3, dadurch gekennzeichnet, dass die Sensormittel in den Gehäusewandungen angeordnete Drahtleitungen (941, 942) umfassen.

5. Datenbehälter nach Anspruch 4, dadurch gekennzeichnet, dass das Gehäuse (11) aussen eine metallische Abschirmung (113) besitzt.

6. Datenbehälter nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Sensormittel einen Druckdetektor (95,951) für den Innendruck (p_i) des Gehäuses (11) umfassen.

7. Datenbehälter nach den Ansprüchen 5 und 6, dadurch gekennzeichnet, dass die Gehäusewandungen (111, 112) mit einem Durchbruch (952) versehen sind, der bei Entfernung der Abschirmung (113) das Gehäuseinnere mit der Atmosphäre verbindet.

8. Datenbehälter nach Anspruch 2, dadurch gekennzeichnet, dass die Zerstörungssensoren in der Gehäusewandung angeordnete Hohlräume (962, 963, 964, 965) umfassen, die paarweise unter demselben Druck (p_1, p_2) stehen, wobei jeweils zwei Hohlraumpaare (962, 963; 964, 965) an zwei Differenzdruckdetektoren (967, 968) angeschlossen sind, deren Ausgangssignale einer Differenzdrucksensorstufe (96) zugeführt sind (Fig. 2).

9. Datenbehälter nach einem der Ansprüche 2 bis 8, dadurch gekennzeichnet, dass die Sensormittel eine Relaisstufe (90) umfassen, die von den Zerstörungssensoren angesteuert ist und die Unbrauchbarmachung der Nutzinformation bewirkt.

10. Datenbehälter nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die Identifikationseinrichtung (40, 70) nur den Auslese-Zugriff zum Hauptdatenspeicher (20) kontrolliert.

11. Datenbehälter nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass er eine zweite Identifikationseinrichtung (30, 60) enthält, die unabhängig von der erstgenannten Identifikationseinrichtung (40, 70) den Einschreibe-Zugang zum Hauptdatenspeicher (20) kontrolliert.

12. Datenbehälter nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass er eine Zeitgeberstufe (50, 51, 53) enthält, die den Zugriff zum Hauptdatenspeicher (20) nur während eines vorgewählten Zeitraums zulässt.

13. Datenbehälter nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass er zum lösbaren Anschliessen an eine Ladeeinrichtung (1000) ausgebildet ist, welche die Nutzdaten vollautomatisch in den Hauptdatenspeicher (20) einschreibt.

14. Datenbehälter nach Anspruch 10 und 13, dadurch gekennzeichnet, dass die Ladeinrichtung (1000) einen Identifikationsdatenspeicher (1130), in welchem die für die zweite Identifikationseinrichtung (30, 60) im Datenbehälter (1) nötigen Identifikationsdaten gespeichert sind, sowie Mittel zur automatischen Eingabe dieser Identifikationsdaten in die zweite Identifikationseinrichtung (30, 60) umfasst.

15. Anwendung des Datenbehälters nach einem der vorangehenden Ansprüche zur Speicherung von Schlüsseldaten bei Chiffriersystemen.

16. Anwendung des Datenbehälters nach einem der vorangehenden Ansprüche zur Speicherung von Schlüsseldaten bei Identifikationssystemen.

DR. BERG DIPL.-ING. STAPF
DIPL.-ING. SCHWABE DR. DR. SANDMAIR
PATENTANWÄLTE
Postfach 860245 · 8000 München 86

3023427

4

Anwaltsakte: 30 945

23. Juni 1980

GRETAG Aktiengesellschaft

8105 Regensdorf/Schweiz

Mobiler Datenbehälter

☎ (089) 988272
988273
988274
983310

Telegramme:
BERGSTAPFPATENT München
TELEX:
0524560 BERG d

Bankkonten: Hypo-Bank München 4410122850
(BLZ 70020011) Swift Code: HYPO DE MM
Bayer. Vereinsbank München 453100 (BLZ 70020270)
Postscheck München 65343-803 (BLZ 70010080)

Case 7-12412/GTS 444/+

Mobiler Datenbehälter

Die Erfindung betrifft einen mobilen Datenbehälter zur gegen unbefugten Zugriff gesicherten Speicherung von Nutzdaten mit einem abgeschlossenen Gehäuse, in welchem sich ein Hauptdatenspeicher für die Nutzdaten und eine Identifikationseinrichtung befinden, welche ihr von aussen zugeführte Identifikationsdaten mit in ihr gespeicherten Identifikationsdaten vergleicht und je nach Vergleichsergebnis den Zugang zum Hauptdatenspeicher freigibt oder blockiert, und welcher Datenbehälter ferner mit Sensormitteln ausgestattet ist, die bei gewaltsamem oder unbefugtem Oeffnen des Datenbehälters einen Teil der gespeicherten Daten unbrauchbar machen oder zerstören.

Die sichere Aufbewahrung von Daten aller Art bzw. die Sicherung der Daten gegen unbefugten Zugriff gewinnt zunehmend an Bedeutung. Bei stationären Anlagen, wie z.B. in Banken und Tresor- oder Computerräumen, erfolgt die Sicherung gegen unbefugten Datenzugang hauptsächlich durch Einlagerung der Daten in Räume mit massiven Wänden, Ueberwachung der Räume mittels verschiedener Alarmsysteme und/oder durch entsprechendes Personal und durch verschiedene mehr oder weniger komplizierte Identifizierungssysteme, die den Zugang automatisch nur dazu Befugten gestatten. Diese Massnahmen sind jedoch für mobile Datenbehälter, die vielfach möglichst klein und leicht sein sollen bzw. müssen, im allgemeinen unpraktikabel.

Für viele Anwendungszwecke eines solchen Datenbehälters, insbesondere beispielsweise im diplomatischen Nachrichtenverkehr oder als Schlüsselspeicher für Chiffriersysteme, kann eher in Kauf genommen werden, dass die gespeicherten Daten gelöscht bzw. zerstört werden, als dass sie Unbefugten in die Hände gelangen.

Aufgabe der Erfindung ist demnach, einen mobilen Datenbehälter zu schaffen, der keinen Zugang zu den in ihm enthaltenen Daten für Unbefugte zulässt. Insbesondere soll dieser Datenbehälter keine massiven Wände und dergleichen benötigen, sodass er entsprechend klein und leicht ausgebildet sein kann, und keine Ueberwachung durch irgendwelches Personal erfordert. Ferner sollen die in ihm gespeicherten Daten zerstört oder unbrauchbar gemacht werden, wenn der Behälter unbefugt oder gewaltsam geöffnet wird.

Diese der Erfindung zugrundeliegende Aufgabe wird erfindungsgemäss durch die im Anspruch 1 aufgeführten Massnahmen und Merkmale gelöst.

In der DE-OS 2 224 937 ist ein Identifikationssystem mit Datenträgern beschrieben, auf denen Identifikationsdaten und irgendwelche anderen, z.B. ein Bankkonto des Benützers betreffende Daten gespeichert sind, wobei letztere durch die Identifikationsdaten gesichert sind. Die Datenspeicher sind durch ein Sensorsystem gegen körperlichen Zugriff geschützt, indem dieses System bei einem Zugriffsversuch automatisch und zwangsläufig die Identifikationsdaten löscht. Auf diese Weise wird zwar der Datenträger als Identifikationsmittel unbrauchbar und wertlos, die übrigen gespeicherten Daten bleiben jedoch erhalten und können daher in unbefugte Hände geraten. Diese bekannten Datenträger sind daher zur Lösung der ~~der~~ Erfindung zugrundeliegenden Aufgabe ungeeignet.

Im folgenden wird die Erfindung anhand der Zeichnung näher erläutert. Es zeigen:

Fig. 1 eine schematische Schnittdarstellung eines erfindungsgemässen Datenbehälters mit einem Blockschema der in ihm enthaltenden elektronischen Funktionsgruppen,

Fig. 2-4 diverse Details aus Fig. 1 in schematischer Darstellung,

Fig. 5 eine schematische Schnittdarstellung einer Ladevorrichtung zum Einspeichern von Daten in den Behälter, und

Fig. 6 eine schematische Darstellung einer mit dem Behälter ausgerüsteten Identifiziereinrichtung.

Der in Fig. 1 als Ganzes mit 1 bezeichnete Datenbehälter umfasst ein Gehäuse 11 mit einem beispielsweise wannenförmigen Unterteil 111 und einem ebenen Deckel 112. Das Gehäuse besteht aus nicht leitendem Kunststoff und ist aussen allseits mit einer Metallschicht 113 umgeben.

Im Datenbehälter 1 befinden sich u.a. ein Hauptdatenspeicher 20, ein Zentralidentifikationsdatenspeicher 30 und ein Teilnehmeridentifikationsdatenspeicher 40. Jedem dieser drei Speicher ist eine Speichersteuerung 21 bzw. 31 bzw. 41, eine Löscheinrichtung 22 bzw. 32 bzw. 42 und ein Schreibtor 23 bzw. 33 bzw. 43 zugeordnet. Ueber die Schreibtore können dem Datenbehälter 1 via an seinem Gehäuse 11 vorgesehene Steckanschlüsse S_1 bzw. S_2 bzw. S_3 Daten zugeführt und in die Speicher geladen werden. Die Zuordnungen der Daten zu den einzelnen Speicherplätzen usw. besorgen dabei die Speichersteuerungen, die ihrerseits über einen Mehrfach-Steckanschluss G in der Gehäusewand des Behälters die nötigen Steuerbefehle, wie etwa Umschalten von Lesen auf Schreiben etc., erhalten. Die Speichersteuerungen umfassen im wesentlichen einen Adresszähler und einen Adressdekodierer und sind daher nicht näher detailliert.

Ferner ist im Datenbehälter eine quarzgesteuerte Uhr 50 mit einem Untersetzer 51 für den Uhrentakt, einer Stellstufe 52 zur Verstellung bzw. Korrektur der Uhr 50 und einem mit der Uhr zusammenarbeitenden Zeitschalter 53 vorgesehen. Die Stellstufe 52 und der Zeitschalter 53 sind von zwei Steckanschlüssen U bzw. Z an der Behälterwand aus ansteuerbar. Die Ansteuerung des Zeitschalters 53 ist durch ein in seiner Verbindungsleitung zum Steckanschluss eingeschaltetes Tor 54 gesichert.

Mit den beiden Identifikationsdatenspeichern 30 und 40 arbeiten zwei Vergleichsstufen 60 bzw. 70 zusammen. Diese erhalten einerseits Daten aus den beiden Speichern 30 und 40 und anderseits über

einen Zentralenidentifikationsdatensteckanschluss ZI bzw. über ein Tor 71 über eine in der Gehäusewand angeordnete Eingabetastatur 72 für Teilnehmeridentifikationsdaten. Anstatt über die Tastatur 72 kann der Vergleichsstufe 70 auch über einen Teilnehmeridentifikationsdatensteckanschluss TI Identifikationsinformation von aussen zugeführt werden. Dieser kann sowohl anstelle der Tastatur bei der teilnehmerseitigen Identifikation, aber auch, wie noch beschrieben wird, während der Identifikation durch die Ladezentrale benutzt werden.

Der Teilnehmeridentifikationsdatenspeicher 40 enthält neben noch zu erläuternden Teilnehmeridentifikationsdaten noch eine für den Datenbehälter 1 spezifische Information, z.B. eine Laufnummer. Diese Information ist so gespeichert, dass sie über einen weiteren Steckanschluss L direkt auslesbar ist.

Die Vergleichsstufe 70 steuert das Tor 43 und ein Lese-Tor 24 an, welches den Datenfluss vom Hauptdatenspeicher 20 zu einem Lese-Steckanschluss L_1 kontrolliert. Dieses Lese-Tor 24 wird gleichzeitig auch vom Zeitschalter 53 angesteuert. Ein Alarmausgang der Vergleichsstufe 70, an dem das Vergleichsergebnis signalisiert wird, ist mit einem entsprechenden Steckanschluss A_2 am Behälter 11 verbunden.

Die Vergleichsstufe 60 blockiert bzw. öffnet die Schreib-Tore 23 und 33, das Tor 54 und die Stellstufe 52 für die Uhr 50. Ferner besitzt diese Stufe 60 einen Alarmausgang, der mit einem entsprechenden Steckanschluss A_2 in der Behälterwand verbunden ist.

Ferner ist im Datenbehälter noch eine Mischstufe 80 und in der Zuleitung vom Speicher 30 zur Mischstufe eine steckbare Brücke 81 vorgesehen, welch letztere normalerweise offen ist. Bei eingesteckter Brücke werden die aus dem Hauptdatenspeicher 20 und dem Zentralidentifikationsdatenspeicher 30 ausgelesenen Daten miteinander z.B. Modulo-2 vermischt. Das Mischprodukt gelangt über das Lese-Tor 24 an den Leseanschluss L_1. Bei nicht eingesteckter bzw. offener

Brücke 81 können die Zentralidentifikationsdaten nicht zur Mischstufe 80 gelangen. In diesem Falle gelangen dann die aus dem Hauptdatenspeicher 20 ausgelesenen Daten unvermischt an den Lese-Anschluss L_1.

Mittels einer weiteren Brücke 82 können, wie noch weiter unten erläutert wird, im Bedarfsfalle die Ausgänge der beiden Vergleichsstufen 60 und 70 zusammengeschaltet werden.

Ferner befinden sich im Datenbehälter 1 eine Relaisstufe 90, die von verschiedenen, noch zu erläuternden Zerstörungssensoren angesteuert ist, und eine Stromquelle 100 z.B. in Form eines wiederaufladbaren Akkumulators. Die Stromquelle 100 ist mit zwei weiteren Steckanschlüssen B_1 und B_2 an der Gehäusewand verbunden.

Die Relaisstufe 90 steuert drei Schaltkontakte 91-93. Im Ruhezustand der Relaisstufe 90, welcher deren Normalzustand entspricht, befinden sich die Schaltkontakte in der gezeigten Stellung. Dabei werden über die Kontakte 92 und 93 den Speichern 20 bis 40 bzw. deren zugeordneten Steuerungen 21-41 die Speisespannung von der Stromquelle 100 und der Systemtakt T vom Untersetzer 51 zugeführt. Der Kontakt 91 ist offen. Bei Ansprechen der Relaisstufe 90 werden die Kontakte in ihre nicht gezeigte Stellung übergeführt. Dabei sind die Spannungs- und die Taktzufuhr für die Speicher unterbrochen und über den Kontakt 91 wird den den Speichern 20-40 zugeordneten Löscheinrichtungen 22-42 Speisespannung zugeführt. Je nach Art der Speicher bewirkt die Unterbrechung der Speicherspeisung und/oder die Aktivierung der Löscheinrichtungen die Zerstörung bzw. Löschung der gespeicherten Daten.

Als Speicher kommen bevorzugt solche mit nichtbewegten Speichermedien, wie RAM-Speicher, CCD-Speicher oder Magnetblasenspeicher in Frage, jedoch können auch Magnetbandspeicher oder Magnetplattenspeicher eingesetzt werden.

Die Löscheinrichtungen hängen natürlich von der Art der zur Anwendung gelangenden Speicher ab. Im Falle von Magnetblasenspeichern z.B. können die Löscheinrichtungen gemäss Fig. 3 aus einer Spule 221 bestehen, die ein genügend starkes Magnetfeld zu erzeugen imstande

ist, welches die gespeicherten Daten zerstört. Bei anderen Speichern, die ihre Ladung bei Speisespannungsausfall ebenfalls nicht automatisch verlieren, können die Löscheinrichtungen z.B. aus einer kleineren Steuerung bestehen, welche in rascher Folge alle Speicherplätze mit der gleichen Information, z.B. mit lauter binären Nullen lädt. Im Falle von flüchtigen Speichern, die die gespeicherte Information bei Speisespannungsausfall und/oder Taktausfall verlieren, kann natürlich auf die Löscheinrichtungen auch verzichtet werden.

Die drei Speicher 20-40 könnten selbstverständlich auch durch Bereiche eines einzigen grösseren Speichers gebildet sein und z.B. auch selbst wieder in mehrere Speicherblöcke aufgeteilt sein. Auch könnten die drei Speichersteuerungen 21-41 durch eine einzige, entsprechend kompliziertere Steuerung realisiert sein. Die dargestellte Drei-Teilung wurde lediglich aus Gründen der besseren Anschaulichkeit gewählt.

Die Relaisstufe 90 wird von hier z.B. drei Sensorstufen 94-96 angesteuert, die ihrerseits mit entsprechenden Fühlern bzw. Gebern, die im Inneren des Datenbehälters bzw. in dessen Wänden angeordnet sind, zusammenarbeiten.

Die Sensorstufe 94 ist ein Stromdetektor. Die zugehörigen Fühler sind als dünne Drahtleitungen 941 und 942 ausgebildet, die in den Wänden des Behälters verlegt sind und über Vorwiderstände 943 und 944 an die Spannungsquelle 100 angeschlossen sind. Der Verlauf der Drahtleitungen in den Behälterwänden ist von Behälter zu Behälter verschieden und vorzugsweise zufallsmässig gewählt. An den Uebergangsstellen zwischen dem Behälterunterteil 111 und dem Deckel 112 sind die Leitungen durch Steckverbindungen 945 und 946 verbunden. Falls durch eine äussere Einwirkung eine der Leitungen irgendwo unterbrochen wird, bringt die Stromsensorstufe 94 die Relaisstufe 90 zum Ansprechen und veranlasst dadurch die schon weiter oben geschilderten Vorgänge zur Datenlöschung.

Die Sensorstufe 95 wird von einem Druckfühler 951 angesteuert, der auf den im Datenbehälter 11 herrschenden Innendruck p_i reagiert. Die Sensorstufe 95 bringt die Relaisstufe 90 zum Ansprechen, wenn der Innendruck z.B. infolge gewaltsamen Oeffnens des Datenbehälters um einen bestimmten Betrag von einem Sollwert abweicht.

An irgendeiner Stelle in der Behälterwand, z.B. hier im Boden, ist die Kunststoffwand mit einem Durchbruch 952 versehen, der jedoch durch die Metallabschirmung 113 hermetisch abgeschlossen ist. Falls die Metallabschirmung aus irgendeinem Grunde entfernt wird, führt dies zu einer Druckveränderung im Datenbehälter und damit zum Ansprechen der Relaisstufe 90.

Die Sensorstufe 96 arbeitet mit einer Vielzahl von Differenzdruckfühlern 961 zusammen, von denen in Fig. 1 nur zwei dargestellt sind. Diese Differenzdruckfühler 961 erfassen die Drücke in jeweils vier an sie angeschlossenen Kanälen 962-965 in den Behälterwandungen. Diese Kanäle, die jeweils paarweise unter demselben Druck stehen, verlaufen willkürlich innerhalb der Behälterwand.

In Fig. 2 ist ein solcher Differenzdruckfühler 961 näher dargestellt. Er enthält im wesentlichen zwei z.B. piezo-elektrische Druckaufnehmer 966, die je einen der vier Kanäle 962-965 abschliessen, und zwei jeweils an die zwei zu einem Kanalpaar 962-964 bzw. 963-965 gehörenden Druckaufnehmer angeschlossene Differenzverstärker 967 und 968, deren Ausgänge über nicht näher bezeichnete Leitungen und Steckverbindungen mit der Sensorstufe 96 verbunden sind.

Im Kanalpaar 962-964 herrscht jeweils der Druck p_1, im Kanalpaar 963-965 ein dazu verschiedener Druck p_2. Im Normalfall werden also die Ausgangssignale beider Differenzverstärker 968 und 967 gleich Null sein.

Wird nun z.B. infolge gewaltsamen Oeffnens des Datenbehälters irgendeiner der Kanäle aufgebrochen, so findet Druckausgleich mit der Umgebung statt und der oder die Differenzverstärker kommen aus dem Gleichgewicht. Dies wird dann von der Sensorstufe 96 entsprechend ausgewertet und führt schliesslich zum Ansprechen der Relaisstufe 90.

Durch die paarweise Anordnung von Kanälen in Verbindung mit den Differenzverstärkern haben z.B. durch Temperaturschwankungen bedingte Druckdrifterscheinungen keinen Einfluss auf die Funktion dieser Stufe. Durch die Verwendung von jeweils zwei Kanalpaaren unter verschiedenen Drücken ist es auch ausgeschlossen, den Behälter unbefugt in einem Raum zu öffnen, in dem derselbe Druck wie in einem der Kanäle herrscht.

Die Kanäle können als Hohlräume innerhalb der Kunststoffwände des Datenbehälters ausgebildet sein. Genausogut ist es aber auch möglich, die Kanäle durch Schläuche oder Rohrleitungen zu bilden, die in die Behälterwand eingegossen sind. In letzterem Fall bestehen die Schläuche bzw. Rohrleitungen vorzugsweise aus demselben oder einem chemisch und physikalisch ähnlichen Material wie die Behälterwand, sodass es z.B. nicht möglich ist, durch chemisches oder physikalisches Abtragen Zugang zu den Kanälen zu erhalten, ohne diese zu zerstören.

Die diversen Zerstörungssensoren (Leitungen, Kanäle etc.) sind, wie schon gesagt, von Behälter zu Behälter verschieden und vorzugsweise zufallsmässig verteilt in den Behälterwänden angeordnet. Dies kann z.B. mittels über einen Zufallsgenerator gesteuerter Bearbeitungsmaschinen erfolgen. Auf diese Weise ist gewährleistet, dass keine zwei Behälter bezüglich dieser Sensoren gleich ausgebildet sind und somit die Sicherheit bezüglich unbefugten Oeffnens wesentlich grösser ist.

Die metallische Abschirmung 113 des Datenbehälters 1 soll verhindern, dass Lage und Verteilung der Zerstörungssensoren mittels radiographischer Methoden herausgefunden werden können.

Nebst den drei geschilderten Zerstörungssensoren können selbstverständlich auch noch Sensoren anderer Art vorgesehen sein. So wäre es beispielsweise gemäss Fig. 4 ohne weiteres möglich, an einem oder an mehreren Stellen in der Behälterwand 111 einen Schwingkreis 971 anzubringen, der mit einer entsprechenden Detektorstufe 97 zusammenarbeitet. Der Schwingkreis würde sich bei Annäherung oder z.B. bei Entfernung der metallischen Abschirmung 113 verstimmen und dadurch über die Detektorstufe 97 die Relaisstufe 90 zum Ansprechen bringen.

Wie in Fig. 1 durch die strichlierten Linien 921 und 931 angedeutet ist, wäre es auch möglich, die Takt- und/oder die Speiseleitungen zu den Speichersteuerungen durch die Behälterwände führen, wodurch eine weitere Sicherung erreicht würde.

In Fig. 5 ist eine zum Laden von Daten in den Datenbehälter 1 bzw. dessen Speicher besonders geeignete Ladezentrale 1000 dargestellt. Sie umfasst ein massives Behältnis 1001 mit einem wannenförmigen Unterteil 1011 und einem Deckel 1012. Das Gehäuse ist gegen Zugang durch Unbefugte mittels irgendwelcher konventioneller Massnahmen, die hier lediglich durch einen Schlüssel 1013 symbolisiert sind, geschützt.

Im Inneren des Behältnisses 1001 befinden sich im wesentlichen ein Datensteuer-Computer 1100 und eine hier nur durch eine strichpunktierte Linie angedeutete Steckverbindung 1101 für ein oder mehrere Datenbehälter 1, 1' etc. Ferner sind eine Stromquelle 1200, ein mit dem Deckel 1012 zusammenarbeitender Schaltkontakt 1201, eine Oder-Stufe 1300, ein akustischer Alarmgeber 1301 und für jeden Datenbehälter ein optischer Alarmgeber 1302 vorgesehen.

Der Datensteuer-Computer 1100 ist irgendein herkömmlicher Computer und enthält u.a. eine Datenquelle 1110, über die noch zu sprechen ist, und pro anzuschliessenden Datenbehälter 1 einen Zentralenidentifikationsdatenspeicher 1130 und einen Teilnehmeridentifikationsdatenspeicher 1140. In diesen beiden Speichern 1130 und 1140 sind für sämtliche zum System gehörenden Datenbehälter die individuellen Zentralen- und Teilnehmeridentifikationsdaten gespeichert.

Im folgenden wird die Funktions- und Betriebsweise des Datenbehälters 1 und der Ladezentrale 1000 beschrieben. Dabei wird davon ausgegangen, dass der Behälter bereits von einem früheren Ladevorgang Daten enthält, welche nunmehr ersetzt werden sollen.

Der Datenbehälter 1 wird dazu in die Ladezentrale 1000 eingebracht und über die Steckverbindung 1101 an den Computer 1100 angeschlossen. Der Computer 1100 wird erst freigegeben, wenn der Deckel 1012 der Ladezentrale geschlossen ist, da er, wie hier symbolisch angedeutet ist, erst dann über den Kontakt 1201 mit Speisespannung versorgt wird. Auf diese Weise ist gewährleistet, dass während der Ladung der Datenbehälter keine unbefugten Manipulationen vorgenommen werden können.

Als erstes liest nun der Datensteuercomputer 1100 über den Ausgang L jedes Behälters 1, 1' etc. die Laufnummer der betreffenden Datenbehälters aus dessen Speicher 40 aus. Anhand dieser Laufnummer werden nun aus der Gesamtheit der in den Speichern 1130 und 1140 vorhandenen Identifikationsdaten die dem jeweiligen Behälter zugeordneten ausgewählt und zunächst über den Anschluss ZI die Zentralenidentifikationsdaten in den Vergleicher 60 des jeweiligen Behälters 1 transferiert. Dieser vergleicht nun diese Daten mit den im behälterinternen Speicher 30 enthaltenen Daten. Das Vergleichsergebnis wird über den Anschluss A_1 an den Computer gemeldet, wobei im Falle der Uebereinstimmung im Datenbehälter die Schreibtore 23 und 33 freigegeben werden. Bei Nichtübereinstimmung spricht der akustische Alarm 1301

sowie der dem betreffenden Datenbehälter zugeordnete optische Alarm 1302 an und jede weitere Operation wird unterbunden, was hier durch die Tore 1131 angedeutet ist.

Bei Uebereinstimmung der in der Zentrale und der im Behälter gespeicherten Zentralenidentifikationsdaten wird über den Anschluss S_2 der Speicher 30 im Datenbehälter 1 und der diesem Behälter zugeordnete Speicherbereich des Speichers 1130 in der Zentrale mit einer neuen, z.B. von einem im Datensteuercomputer enthaltenen Zufallsgenerator erzeugten, rein zufälligen Zentralenidentifikationsinformation geladen.

Als nächstes erfolgt für jeden Datenbehälter die Ueberprüfnng der Teilnehmeridentifikationsdaten. Diese werden aus dem durch die Behälterlaufnummer definierten Bereich des Speichers 1140 über den Anschluss TI des Behälters zu dessen Vergleicherstufe 70 transferiert und dort mit den aus dem behälterinternen Speicher 40 ausgelesenen Daten verglichen. Bei Nichtübereinstimmung wird in ähnlicher Weise wie für die Zentralenidentifikationsdaten über die Ausgänge A_2 ein Alarm ausgelöst. Bei Uebereinstimmung werden die Tore 43 und 24 im Behälter 1 freigegeben und es werden neue, zufallsmässig erzeugte Teilnehmeridentifikationsdaten über den Anschluss S_3 des Behälters 1 in dessen Speicher 40 sowie in den durch die Laufnummer definierten Bereich des Speichers 1140 des Datensteuer-Computers 1100 eingelesen.

Für einfachere Anwendungsfälle, in denen die Sicherheit nicht so hoch sein muss, kann auf die Ueberprüfung der Teilnehmeridentifikationsdaten in der Ladezentrale auch verzichtet werden. In diesem Falle müssten einfach die Verbindungen des Computers zu den Anschlüssen S_3 und TI der Behälter unterbrochen werden, was in der Zeichnung durch die Brücken 1102 und 1103 angedeutet ist.

Nach diesen vorbereitenden Kontrolloperationen werden die Hauptdaten über den Anschluss S_1 in den Hauptdatenspeicher 20 jedes Datenbehälters geladen. Die Hauptdaten stammen aus der Datenquelle 1110. Die Datenquelle kann irgendein speicherndes Eingabegerät sein, mittels welchem Daten zur Verfügung gestellt werden können. Falls die Hauptdaten Geheimschlüssel im Zusammenhang mit einem Chiffriersystem sind, kann die Datenquelle auch ein Zufallsgenerator oder dgl. sein, der diese Schlüsseldaten automatisch erzeugt.

Während der diversen Kontroll- und Ladevorgänge werden gleichzeitig auch über die Anschlüsse B_1 und B_2 die Akkumulatoren 100 in den Datenbehältern 1 nachgeladen.

Nach dem Laden des Hauptdatenspeichers 20 wird, falls erforderlich, über den Anschluss U die Uhr 50 im Datenbehälter gestellt und eventuell, über den Anschluss Z, die Zeitgeberstufe 53 gesetzt. Durch letzteres kann ein Zeitfenster festgelegt werden, innerhalb von welchem die Hauptdaten ausgelesen werden können bzw. müssen.

Damit ist der Ladevorgang in der Ladezentrale beendet und die Datenbehälter gelangen nun an den Benützer. Dieser kann lediglich die Hauptdaten aus dem Speicher 20 über den Leseanschluss L_1 auslesen. Er kann jedoch die Daten in den Speichern oder die Einstellung der Zeitgeberstufe 53 nicht verändern, da die entsprechenden Eingänge durch die Zentralenidentifikationsdatenvergleichsstufe 60 blockiert sind.

Um sich Zugriff zu den Hauptdaten zu verschaffen, muss der Benützer zunächst die dem betreffenden Datenbehälter zugeordneten Teilnehmeridentifikationsdaten über die Tastatur 72 in die Vergleichsstufe 70 eingeben. Diese vergleicht die eingegebenen Daten mit den im Speicher 40 gespeicherten Daten und gibt im Uebereinstimmungsfalle das Lesetor 24 und damit den Zugriff zum Hauptdatenspeicher 20 frei. Sofern auch die Zeitgeberstufe 53 das Lesetor 24 freigibt, d.h., sofern der gewünschte Datenzugriffsmoment innerhalb des von der Zeitgeberstufe 53 vorgegebenen Zeitfensters liegt, können dann die Haupt-

daten aus dem Speicher 20 über den Anschluss L_1 ausgelesen werden. Die dazu notwendige Vorbereitung und Ansteuerung der Speicher erfolgt, wie bei allen anderen Operationen, über den Steueranschluss G.

Die Tastatur 72 bzw. die Vergleichsstufe 70 kann so ausgebildet sein, dass z.B. bei dreimaliger Eingabe falscher Identifikationsdaten jede weitere Eingabe blockiert und ein Alarm ausgelöst wird. Auf diese Weise wird verhindert, dass die ihm unbekannten Identifikationsdaten von einem Unbefugten durch systematisches Ausprobieren herausgefunden werden können.

Der elektrische Zugriff zu den gespeicherten Daten über die von aussen zugänglichen Steckanschlüsse des Datenbehälters ist somit durch die zentralen- und teilnehmerspezifischen Identifikationsdaten abgesichert. Der Zugriff durch gewaltsames Oeffnen des Datenbehälters wird durch die diversen Zerstörungssensoren und die mit ihnen zusammenarbeitenden Stufen verhindert.

Eine weitere Sicherheit gegen unbefugten Datenzugriff bildet die Mischstufe 80. Diese vermischt die Hauptdaten mit den Zentralenidentifikationsdaten des Speichers 30, sodass die am Ausgang L_1 entnehmbaren Daten ein Mischprodukt bilden. Bei Anwendung des Datenbehälters als Schlüsselspeicher in Chiffriersystemen kann dann dieses Mischprodukt als Chiffrierschlüssel verwendet werden, sofern die ja ohnehin zufallsmässig erzeugten und dabei unbekannten Zentralenidentifikationsdaten für alle beteiligten Schlüsselbehälter gleich sind. Unter diesen Voraussetzungen ist es dann z.B. möglich, bei unbefugtem Oeffnen des Behälters nur den Zentralenidentifikationsdatenspeicher zu löschen, nicht aber den Hauptdatenspeicher, da die in diesem enthaltenen Daten ohne die Zentralenidentifikationsdaten ohnehin unbrauchbar und demnach wertlos sind.

Für besonders wichtige Anwendungen kann es zweckmässig sein, die sicher zu speichernden Daten nicht im Klartext, sondern in irgendeiner Weise chiffriert oder sonstwie verarbeitet zu speichern. In Fig.1

ist daher ein Prozessor 83 strichliert angedeutet, der in die Datenwege vom Schreibtor 23 zum Speicher 20 und von diesem zum Mischer 80 eingeschaltet ist und vom Steuereingang G aus angesteuert werden kann. Dieser Prozessor chiffriert die zugeführten Hauptdaten mit einem ihm eigenen Chiffrierprogramm und dechiffriert die ausgehenden Daten wieder. Das Chiffrierprogramm wird vom Prozessor aufgrund einer in ihm gespeicherten Schlüsselinformation erzeugt, welche beim Laden des Datenbehälters in den Prozessor geladen wird. Die Vorbereitung des Prozessors dazu erfolgt wie bei den Speichern über den Steueranschluss G am Datenbehälter 1.

Falls die Datenbehälter zur Speicherung von Chiffrierschlüsseln dienen, müssen natürlich alle zu einem Verbindungsnetz gehörenden Schlüsselbehälter gleichzeitig geladen werden, und zwar für jede Verbindungsmöglichkeit innerhalb des Netzes jeweils paarweise mit derselben Information. In diesem Falle ist die Ladezentrale zur gleichzeitigen Aufnahme von mehreren Datenbehälter ausgebildet. Die diversen Kontrollen und so weiter erfolgen jedoch für jeden einzelnen Behälter separat. Die Laufnummern der einzelnen Behälter bestimmen dann die Zuordnung der einzelnen Schlüsseldaten zu den jeweiligen Behältern.

Die in Fig. 1 als offen bzw. unterbrochen strichliert angedeutete Brücke 82 bietet eine weitere Variationsmöglichkeit des erfindungsgemässen Datenbehälters. Bei geschlossener bzw. eingesetzter Brücke 82 kann nach Identifizierung einer befugten Person mittels der Vergleichsstufe 70 und damit verbundener Freigabe des Schreibtors 23 über den Schreibanschluss S_1 Information in den Datenhauptspeicher 20 eingeschrieben und/oder die Uhr 50 über den Stellanschluss U verstellt werden. Dies kann für gewisse Ausnahmesituationen wünschbar und vorteilhaft sein, bildet aber nicht den Regelfall.

Ausser der Absicherung der gespeicherten Daten durch die schon beschriebenen Mittel ist es z.B. auch möglich, eine weitere Sicherung über die Ausleserate vorzusehen. Dies ist insbesondere im Zusammenhang mit Chiffriersystemen vorteilhaft. So kann z.B. die Steuerung 21

des Hauptdatenspeichers 20 so ausgelegt sein, dass sie im Takt T des vom Untersetzer 51 heruntergeteilten Uhrentaktes und somit autonom von der Uhr 50 gesteuert jeweils nur eine bestimmte Anzahl von Datenbits aus dem Speicher ausgibt. Das Ganze kann dabei auch so organisiert sein, dass die Daten in gewissen, durch die Uhr 50 vorgegebenen Zeitabständen völlig autonom ausgelesen und vorzugsweise die betreffenden Speicherplätze des Hauptdatenspeichers dann sofort nach jeder Ausgabe gelöscht werden.

Das Löschen der jeweils ausgelesenen Daten kann auch bei anderen Anwendungen erwünscht sein. Vorzugsweise sind daher im Datenbehälter Umschaltmittel, z.B. in Form von Steckbrücken oder dgl. vorgesehen, mittels welcher zwischen den Betriebsweisen "Löschen" und "Nicht-Löschen" nach dem Auslesen gewählt werden kann.

Eine typische Anwendung für den erfindungsgemässen Datenbehälter ist sein Einsatz als Geheimschlüsselspeicher in einer Identifikationseinrichtung. Eine solche Einrichtung ist in Fig. 6 schematisch dargestellt.

Die Einrichtung besteht aus zwei lösbar miteinander mechanisch und elektrisch gekoppelten Teilen, und zwar einer Prüfstation 2000 und dem Datenbehälter 1. Die Prüfstation befindet sich an dem Ort, an welchem die Identifikation vorgenommen werden soll, z.B. am Eingang eines Gebäudes oder dgl. Die Prüfstation enthält einen Antrieb 2001 für die zu identifizierenden Kennkarten 2002, zwei Leseköpfe 2003 und 2004 für zwei Kartenspuren 2005 und 2006, zwei mit den Leseköpfen verbundene Verstärker 2007 und 2008 und zwei Dekodierer 2009 und 2010, zwei an die Dekodierer angeschlossene Und-Tore 2011 und 2012, ein weiteres Und-Tor 2013, einen Alarmgeber 2014, eventuell eine Tastaur 2015 und eine alle Funktionsabläufe veranlassende bzw. steuernde zentrale Steuerung 2016.

Der Datenbehälter 1 ist im wesentlichen gleich aufgebaut wie der gemäss Fig. 1. Es sind daher in Fig. 6 nur die funktionswesentlichen Teile dargestellt. Ausser dem schon beschriebenen Speicher 20 und dem Chiffrierrechner 83 enthält der Datenbehälter 1 zusätzlich noch eine Vergleichsstufe 84, welche ihr über einen Eingang KR zugeführte Daten mit vom Chiffrierrechner 83 stammenden Daten vergleichen und über einen Ausgang AL ein das Vergleichsergebnis kennzeichnendes Signal abgeben kann.

Die Kennkarten 2002 tragen auf ihren beiden Lesespuren zwei Informationen, und zwar irgendeine Kartennummer und eine Krypto-Information, die bei der Kartenherstellung aus der Kartennummer durch Chiffrieren mit einem geheimen Schlüssel gebildet wurde. Beim Identifikationsvorgang werden nun diese beiden Informationen von der Karte abgelesen und über die Und-Tore 2011 und 2012 und über die Eingänge KR und NU dem Vergleicher 84 bzw. dem Chiffrierrechner 83 im Datenbehälter 1 zugeführt. Der Speicher 20 enthält den bei der Kartenherstellung benutzten Geheimschlüssel. Mit diesem Geheimschlüssel bildet nun der Chiffrierrechner aus der Kartennummer die Kryptoinformation. Diese gebildete Kryptoinformation wird nun mit der abgelesenen verglichen und die Uebereinstimmung bzw. Nicht-Uebereinstimmung wird via den Ausgang Al von der Alarmeinrichtung 2014 signalisiert. Die Eingabe der Kartennummer kann alternativ auch über die Tastatur 2015 erfolgen.

Bei herkömmlichen Identifizierungssystemen, die nach diesem Prinzip arbeiten, muss für das "Handling" der Geheimschlüssel grosse Sorgfalt aufgewandt werden, z.B. muss der Schlüssel mittels Kurier an die einzelnen Identifizierungsstationen überbracht und dort gegen unbefugten Zugriff gesichert werden. Der Datenbehälter dagegen erfordert keine besonderen Sicherungsmassnahmen und kann z.B. ohne weiteres mit der Post versandt werden. Aus dem Behälter ist keine Geheiminformation entnehmbar, sondern lediglich das "Gut/Schlecht"-Signal.

Leerseite

Nummer: 30 23 427
Int. Cl.²: G 06 F 13/00
Anmeldetag: 23. Juni 1980
Offenlegungstag: 8. Januar 1981

3023427

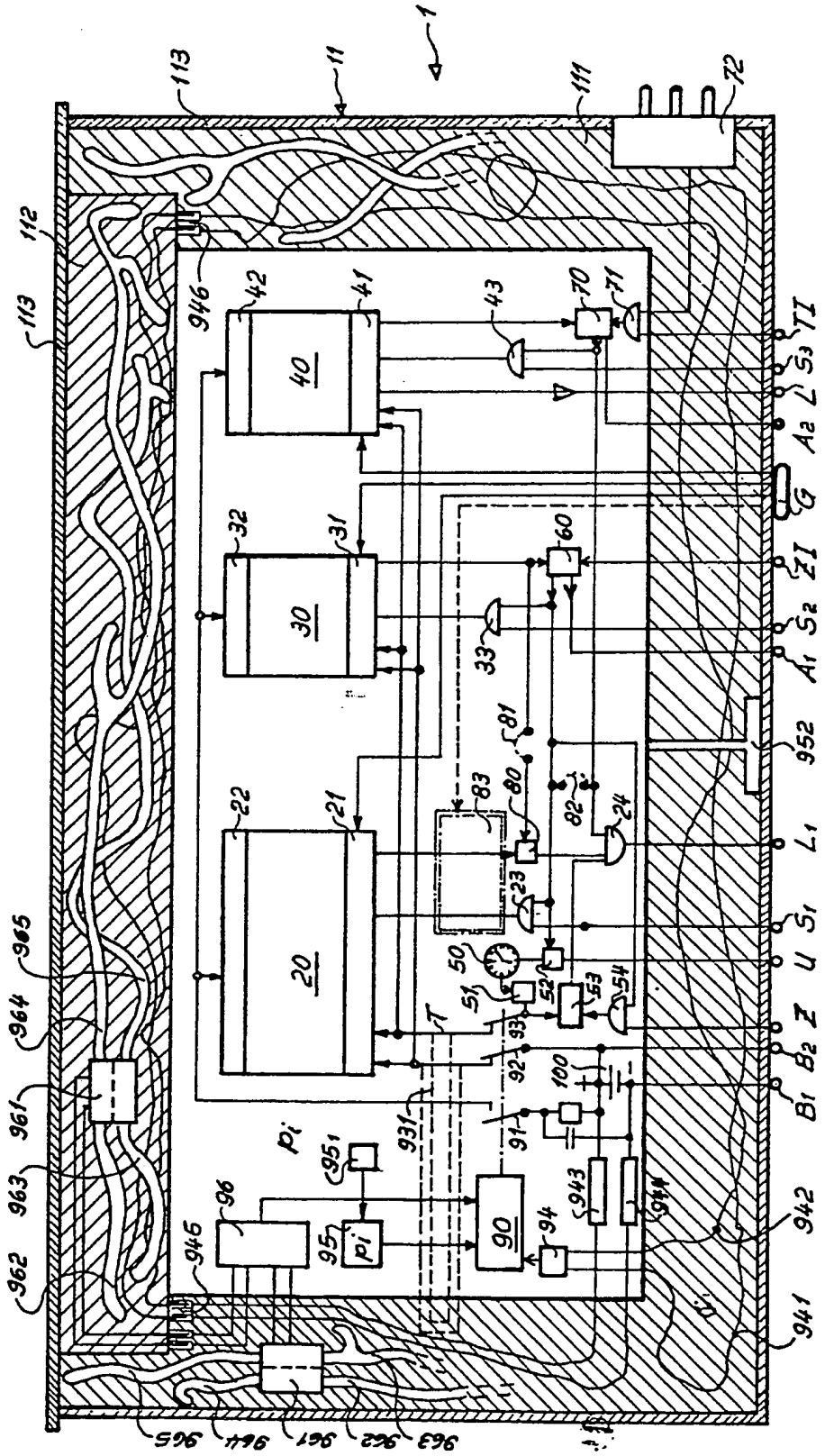


Fig. 1

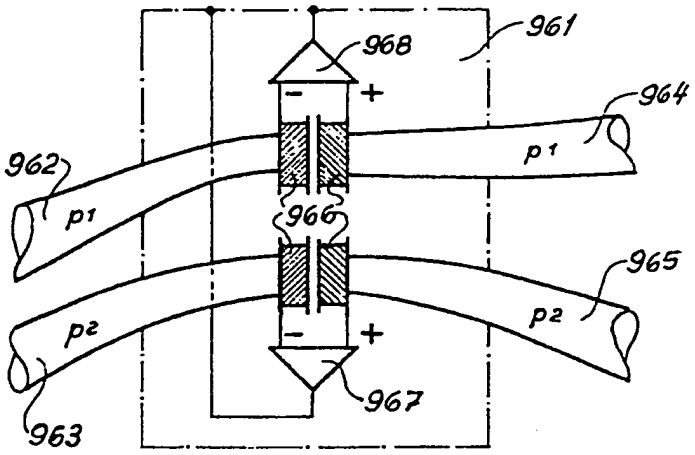


Fig. 2

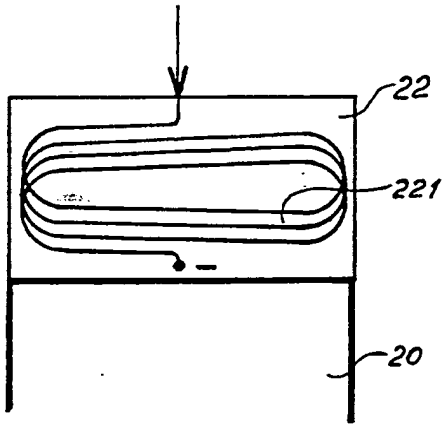


Fig. 3

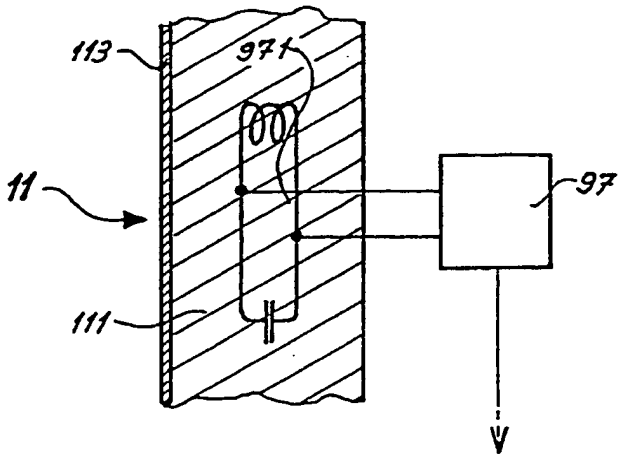


Fig. 4

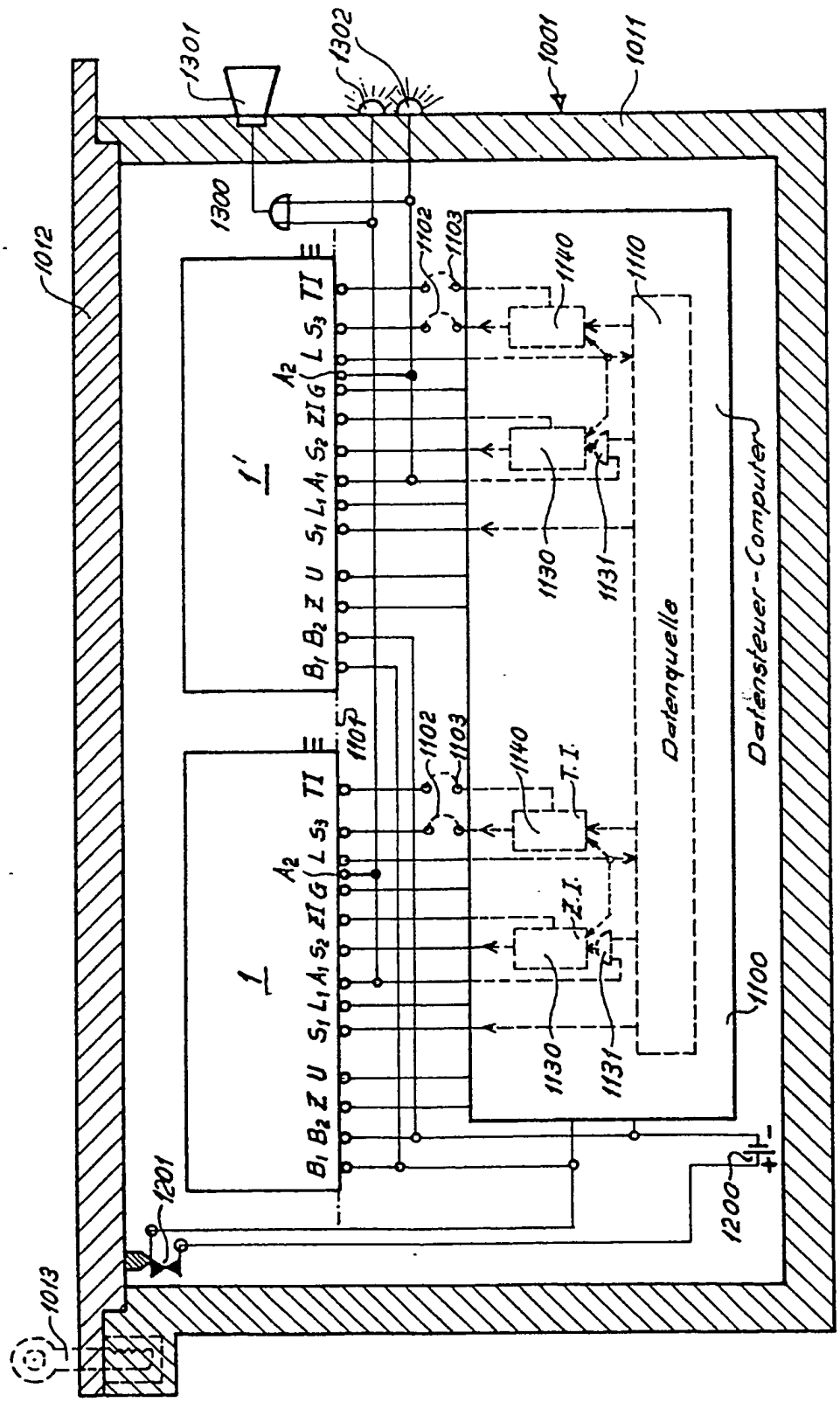

1301
1302
1001
1011
1012
1300
1102
1103
1110
1140
1130
1131
Datenquelle
Datensteuer-Computer
1100
1000
1'
1
B_1 B_2 Z U S_1 L_1 A_1 S_2 ZI G A_2 (L S_3 TI
1107
T.I.
Z.I.
1200
1201
1013

Fig. 5

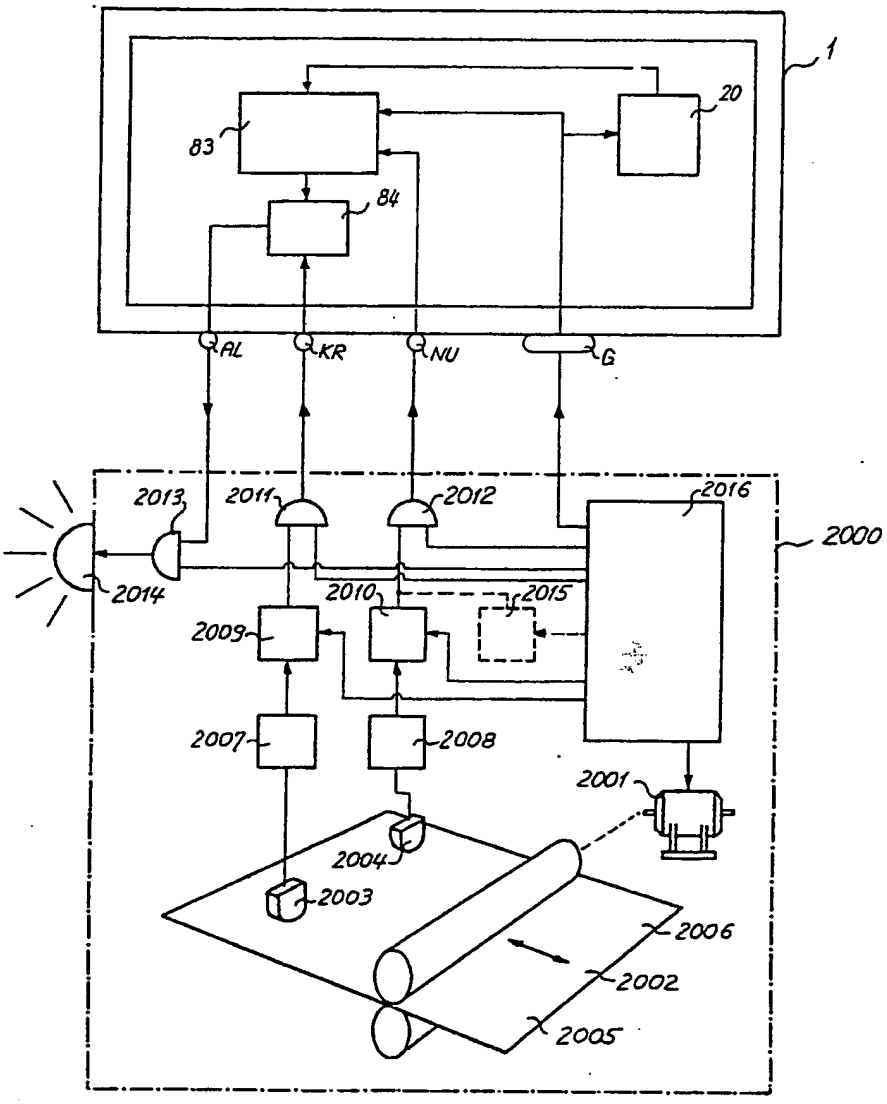

1
20
83
84
AL
KR
NU
G
2000
2013
2011
2012
2016
2014
2010
2015
2009
2007
2008
2001
2004
2003
2006
2002
2005

Fig. 6